15(Q)

TOP SECRET 'U'

TICOM/ I-22

INTERROGATION OF GERMAN CRYPTOGRAPHERS OF THE 'PERS ZS'

DEPARTMENT OF THE AUSWÄRTIGES AMT

This publication is a report on the interrogation of twenty-one cryptographers of 'Pers ZS' carried out in UK at seven meetings during May 1945. 'Pers ZS' worked only on diplomatic systems.

TICOM
2 July, 1945

Copy No. 18
No. of pages:31

Distribution

British
1. Director
2-8 D.D. 3 (7)
9. D.D. 4
10. D.D. (N.S.)
11. D.D. (MW)
12. D.D. (A.S.)
13-14. A.D. (C.C.R.) (2)
15. Col. Leatham

U.S.
32-33. OP20-G(2) (via Lt. Pendergrass)
34. G-2 (via Lt. Col. Hilles)
35-36. S.S.A. (2) (via Major Seaman)
37-38. Director, S.I.D. ETOUSA (2) (via Lt. Col. Johnson)

TICOM
16. Chairman
17-19. S.A.C. (3)
20. Cdr. Bacon
21. Cdr. MacKenzie
22. Cdr. Tandy
23. W/Cdr. Oeser
24. Lt. Col. Johnson
25. Maj Seaman
26. Lt. Eachus
27. Lt. Vance
28. Capt. Cowan
29. Lt. Fehl
30-31. Ticom Files (2)

Additional
39. Dr. Forster
40. Dr. Pickering
41. Lt. Col. Evans
42. Lt. Comdr. Mansen
43. Major G.W. Morgan

TOP SECRET

Interrogation of German Cryptographers

of the 'Pers ZS' Department of the Auswärtiges Amt

Seven meetings were held at which 17 male and 4 female cryptographers were interviewed. The attached Minutes provide a record of the proceedings.

The interrogators were concerned to conceal their own knowledge of the details of the subject and of any specific German or foreign system. The Germans were co-operative and ready to answer questions and volunteer statements.

We know from Ultra sources that Schauffler had been concerned with the cryptographic details of German Diplomatic Cyphers but we did not question him on this subject nor did he speak about it himself.

Interrogation was allowed to develop naturally from such general questions as "What was the nature of your work?" Or questions were put on the captured material we now hold. For example we raised the question of Swedish usage by referring to the Swedish-made Hagelin Machine found among the 'Pers ZS' papers.

The general impression of the party as a Cryptographic Unit was that it was competent but limited. It was seriously handicapped by lack of staff. Hollerith machinery was not introduced until 1942 and then only in small quantities and rather by chance than considered policy. Little or no encouragement came from above and neither directives nor pressure to complete tasks were forthcoming. Liaison with other German Cryptographic Units was very bad and with Allies of Germany non-existent. They were frightened by Machine Cyphers as a practical problem although some theoretical work had been undertaken on the security of such cyphers. They seemed to have relished their low-grade successes unduly and to have been too ready to reject as impossible - and then to forget - the high-grade systems beyond their powers. The senior officers were convinced of the security of German high-grade systems. Virtually no intelligence work was done on the contents of broken messages.

The work of 'Pers ZS' was confined to diplomatic systems and did not include Service Attaché Cyphers. The OKW and Goering's Forschungsamt also worked on Diplomatic systems and the relations of all three stations were marked by jealousy rather than by co-operation.

More can be learned of the German attack on British Diplomatic Systems from Frl. Hagen who is now ill under supervision at Marburg, and we recommend that she be interrogated.

One other member of the party still remains to be interrogated. This is Dr. Helmut Grunsky, a mathematician, who is at present in hospital.

Photographs and finger-prints of all those interrogated are filed in C.C.R. Section G.C.&C.S.

E.R. Vincent,
Acting Chairman for D.D.(4)

4th June, 1945

9th May, 1945 at the Oratory School. First Meeting at 11.30.

Present: Brigadier Tiltman (in the chair), Professor Vincent
Col. Cook U.S.A., Lt. Fehl U.S.A., Dr. Forster
and later: Professor Dr. Rohrbach.

1. It was agreed before the meeting
a. to treat general matters only
b. to interview Professor Rohrbach alone first.

2. Professor Rohrbach was then called and asked to sketch the organisation to which he belonged. It was made clear to him that the meeting had neither the desire nor the power to intimidate him or his colleagues into imparting information against their will. He replied that he and his colleagues were prepared to talk on a professional basis of 'exchange of results' though it was clear to them that the exchange would necessarily be onesided.

3. He gave the official designation of his organisation as Department 'Pers Z S' of the Auswärtiges Amt. It had formerly been known as the 'Chiffrierabteilung' but later the cover 'Pers Z S' was adopted. The organisation was concerned with cryptography on foreign diplomatic codes and cyphers; no military or other material was handled.

4. There was another department of the Auswärtiges Amt which dealt with the production and security of German diplomatic systems, but any liaison between it and 'Pers Z S' was purely informal. This department had remained in B erlin until the end.

5. The head of the organisation was Gesandter SELCHOW. The three sections of which it consisted were under

Oberregierungsrat SCHAUFFLER
" Dr. PASCHKE
" Dr. KUNZE

6. Dr. Kunze was an old hand and been in the organisation for 27 years. He was responsible for the intial breaking of difficult systems, recypherments etc. His staff consisted largely of mathematicians. Hollerith machines had not been available to him until 1942 but by the end he had about 20 machines. This was thought to be due to the personal interest of Ribbentrop.

7. Dr. Paschke was responsible for bookbuilders and translators. His section was organised by countries and languages. He also carried out such liaison as was done with the Wehrmacht.

8. ORR Schauffler: a mathematician. Started life as a schoolmaster, was gassed in the last war and on return to his job found schoolmastering too much for him. Entered this organisation shortly afterwards as a mathematician. Then became interested in Far Eastern languages, in which he specialised. His field was theoretical research ('Grundlagenforschung') on cryptography, and he edited a private periodical which circulated within the office, called 'Schriften des Sonderdienstes'. It was concerned largely with cryptographic methodology. [Comment: Copies found among the documents contained solutions of problems connected with the enigma machine. With this in mind the question of the distribution of the periodical was raised.] It had no distribution outside the office and was only held by senior staff include; a copy went to Selchow, but as he did not understand much about cryptography it was thought improbable that he read it.

9. There was very little liaison with other cryptographic bureaux; nothing was known about relations with foreign cryptographers.

10. Professor Rohrbach was at pains to explain his own position. He had a chair of mathematics at Prague, which he held concurrently with his appointment with the Foreign Office, travelling often back and forth. He had chanced to be at Burgscheidungen when the place was overrun. The senior members of the organisation had panicked in the absence of selchow, and he was the only person who had had the presence of mind to take any common sense action. He had thus become the leader of the party. He was careful to point out that this was not due to any position he held within the organisation or to any superior competence he might have as a cryptographer, but purely to force of character. In discussion of question of cryptographic detail he wished to be regarded merely as a member of Dr. Kunze's section.

11. The gentlemen appeared to be as comfortable as was consistent with the circumstances, but were concerned about one of their number, Dr. GRUNSKY, who was suspected of having acute tuberculosis. This had been discovered the day before they left Germany. It was arranged that he should have a medical examination. [Comment: he has since been admitted to hospital and was therefore not available for interrogation. He is a member of Dr. Kunze's section.]

SECOND MEETING (At 3 o'clock on 9th May 1945 at the Oratory School)

Present: The foregoing and Dr. Kunze, Dr. Paschke and ORR Schauffler

12. The basis on which the meetings were to be conducted was explained to the new arrivals. The principle of 'one-sided exchange' ('einseitiger Austausch') was agreed to. [Comment: The interrogators felt much obliged to Lt.Col. Evans who appears to have been originally responsible for this highly diplomatic formula.]

13. Dr. Kunze was asked to sketch what in his opinion the principal successes of the organisation had been.

14. He stated that he himself had been employed on similar work by the High Command in the last war and mentioned success with British naval cypher at that time.

15. In 1924 he had broken a French system of bigram substitution using 100-figure bigram tables on a 4 figure book.

16. Russian systems had been read at that time but, as Dr. Paschke observed, after the appearance of the British White Paper in 1927 the Russians changed their systems and discouraged circular telegrams; there was then not enough depth.

17. Polish systems consisting of subtractor tables on a 4 figure book were mentioned as having been solved at about that time.

18. In 1929 or 1930 they began to read Jugoslav traffic employing bigrammatic substitution on a 5 girue book. At first the recypherment was applied horizontally, later vertically. Manchurian systems were mentioned, but conversation branched off to the subject of Japanese. At this point ORR. Schauffler also took part in the conversation.

19. Japanese: Until 1934 lower grade Japanese systems were read currently. After 1934 the Japanese went over increasingly to the use of a machine. The moral effect of the machine on the party had been considerable and it was some time before they discovered that it could theoretically be broken. They did not in fact read any traffic until September 1938. They then read the machine currently until February 1939 when it became unreadable owing to difficulties with the wheel turn-over [Comment: The use of a differnt machine does not seem to have been considered]. In the meantime they read all the back traffic as far back as 1936. They continued to read the lower grade material currently until the end.

20. Chinese: ORR. Schauffler had worked on Chinese systems for 20 years, part of the time in conjunction with the celebrated linguist Legationsrat Krebs, whose pupil he considered himself to be. They read 4 figure and 4 letter traffic until 1930. At the beginning of the war Chinese was taken up again in conjunction with the O.K.W., which supplied personnel. It was agreed to discuss Far Eastern traffic in detail at some later meeting.

21. They handled no attaché traffic, either Japanese or any other, Dr. Steinberg of the O.K.W. was said to have worked on Japanese military attaché traffic.

22. British: In 1939 Kunze was approached by the Luftwaffe for assistance with British weather cyphers. He was successful with these.

23. In May 1938 they began to break a British diplomatic system. In 1940 to 41 the tables ran for three months, so that there was considerable depth [Comment: Uncertain whether these two sentences refer to the same system]. They found however that the labour involved was such that it was too much trouble to read the material currently without machines. On the introduction of 'special' keys the investigation was discontinued. A written report was available on this subject [Comment: The circumstance that this investigation was broken off in 1941 and that Hollerith machinery became available in 1942 may be connected, though this point was not raised at the time. They appear at all events to have had no further success with British systems. It was thought best not to press this point for the time being but to discuss it in detail at a later meeting].

24. In 1943 the American strip system No. 2 was solved, but with considerable time lag. It involved a great deal of time and effort. A machine was designed to eliminate this, and Dr. Kunze thought that it must be with the machinery sent from Hermsdorf in three waggons, only one of which had arrived at Zschepplin. He thought that most of the workings on this system had been destroyed at Zschepplin.

25. Italian: Dr. Paschke was asked what success he had had with Italian systems. He replied that he had been instructed in 1935 to devote special attention to Italian and that the results had been the best imaginable; they had read everything ('Den schönsten Erfolg, den man sich denken kann; es wurde alles gelesen'). In 1942-43 work became increasingly difficult: the Italians increased their subtractor material before the collapse and employed bigram substitution over a subtractor over a book. If they had changed the book, the traffic would have become 'impossible' to read. After the collapse they read a Government code 'Impero' recyphered with figures from the encode, with little depth. Later the Government systems were not read for lack of depth, but it was thought that they used double transposition. The Neofascists had used a 5,000 figure subtractor; the peculiar systematic arrangement of the figures in the subtractor assisted solution very much. In the last three months the Neofascists had used unrecyphered books which were easily read, and an alphabetical book with a short subtractor called RA 1.

26. Captured material: When asked what assistance they had had from captured material he said that it was unwelcome and seldom useful. They had never had any liaison with foreign (e.g. Finnish, Hungarian or Japanese) cryptographic organisations and had never been visited by foreign cryptographers.

27. Note: All four gentlemen seemed to be fully cooperative, includ- Dr. Paschke, contrary to reports from the field. They were concerned about their security, as they had no privacy and would in the long run find it difficult to keep the nature of their work secret from their fellow internees. It was suggested that they might be prepared to write reports on their activity, to which all replied that they would be prepared to do so but their present circumstances were unsuited to 'scientific work'.

The meeting was adjourned.

THIRD MEETING

Held at 101 Nightingale Lane, Wandsworth on 10.5.45 at 12.15

Present: Professor Vincent (in the chair), Col. Cook U.S.A., Lt. Fehl U.S.A., Dr. Forster, Frl. Friedrichs
and later: Frl. Dr. Pannwitz, Frau Dr. Hühnke, Frl. Schrader.

28. It was decided before the meeting
a. to discuss general matters only
b. to see Frl. Friedrichs alone first.

29. The basis on which the meetings were to be conducted was explained to Frl. Friedrichs, who agreed. The conversation was conducted in English.

29. Frl. Friedrichs stated that her duty was decypherment of Bulgarian and other Slavonic cyphers. She had, however, from time to time been loaned to other sections. For instance she had been loaned for a time to Dr. Kunze at the time when the American strip system Number 2 was being broken. She had maintained a personal interest in the American strip system and had clearly enjoyed the work very much. She mentioned Herr Zastrow as an authority on U.S. systems.

31. Her approach to the work as a whole was a professional one, the work gave her pleasure and she felt a proprietary interest in it.

32. She touched on the position of women in the organisation. She said it had been a long fight to obtain for women the same pay as men, but that that had finally been achieved, but, though they received the same pay they had not the same status. At the beginning of the war a great many women had been engaged somewhat to the chagrin of men who had not been used to working with large numbers of women. She instanced the case of one woman who had reached a senior position in the organisation, Frl. Hagen, for whom she evidently had a great admiration, and whom she characterised as an extremely able cryptographer. Her duty was primarily British cypher systems and the systems of the Spanish and Portuguese countries. At the time of their departure from Germany Frl. Hagen was in hospital with a skin complaint.

33. When asked whether she knew of any connection that the organisation had with similar organisations outside, she answered in the negative. Such liaison as was done was carried out by Dr. Paschke. She gave the impression that, far from there having been any coordination between the various cryptographic organisations, there was a considerable feeling of rivalry.

34. The general impression that she gave of her organisation was that it was a small, self-contained show, functioning entirely by itself, that it was starved of personnel and equipment and that little interest was taken in it higher up. *

* Total personnel she thought was about 120, of whom 10 were employed in the Slavonic section.

35. The Head of the organisation was a competent administrator who understood little about cryptography, and was content to leave the specialists to run their affairs as it seemed best to them.

36. When asked whether there had ever been any evidence of appreciation of the work done in the organisation, she replied that there had been none. From time to time, copies of the telegrams they issued had been returned to them bearing a stamp indicating that they had been by the Führer, otherwise no indication of the importance attached to this work had penetrated to the level at which she worked.

37. No intelligence was extracted from the material by them, except such as was necessary in order to enable them to continue reading the traffic. There was no sense of urgency in the office, decyphered messages were not transmitted by teleprinter to their recipients.

38. In the matter of translation of decyphered texts, the organisation had established rigid rules and in general favoured a literal translation in contradistinction to the practice of the OKW, which was always concerned to round off and polish up the translation and make it flow, usually leaving out corrupt groups or obscure passages.

39. There was little encouragement given to communication of results inside the organisation by junior members, who were encouraged to mind their own business. In general such exchange of results as was carried out was done on a purely informal basis as between friends.

40. Frl. Friedrichs was concerned about the possible fate of the men. She herself had been about the world a fair amount and would find it easy to obtain different employment after the war. Most of the men were already in late middle age; they had done nothing but cryptography all their lives and had no other interests and she did not see how they were going to support themselves without it. [Comment: No statement was made by the interrogators in response to this hint regarding the eventual disposal of the members of this organisation.]

41. It was felt that little more of a general nature could be elicited, so that it was decided to call in the remaining ladies, Frau Dr. Hühnke, Frl. Dr. Pannwitz and Frl. Schrader. A short discussion on personal matters was held with them. They were concerned about the fate of their men-folk and wished information to be given to their relations in Germany that they were safe and sound if this were possible. It was pointed out that the members of the meeting had no power to do this but were prepared to transmit such requests; they could, however, give no guarantee that anything would be done. None of the ladies appeared any the worse for their two days' sojourn in Holloway Prison.

Intermediate Meeting; held at 101 Nightingale Lane, Wandsworth on 13th May 1945 at 3 p.m.

Present: Dr. Forster; Frl. Friedrichs, Frau Dr. Hühnke, Frl. Dr. Pannwitz

41a. The real object of this meeting was to obtain information on the whereabouts of Frl. Hagen, the specialist on British and South American systems (see para. 32), with a view to evacuating her to a rear area under British or U.S. control. The ostensible object was to bring Frl. Friedrichs' luggage, which had been delivered at the Oratory School in error.

41b. Before the meeting took place, the interrogator was met, on arrival in the German detainees' wing by a young German woman who did not belong to the party he intended to see and was apparently a new arrival. She said: 'Wer sind Sie?' and got the reply that the interrogator was looking for Frl. Friedrichs. She then said: 'Sind Sie vom Auswärtigen Amt?'. The interrogator denied any connexion with the Foreign Office.

41c. Frl. Friedrichs and her party being assembled in a separate room, Frau Dr. Hühnke said that Frl. Hagen was last heard of in the German military hospital at Zschepplin. This hospital was housed in the Schloss, the same building as was occupied by the 'Pers.ZS' personnel. She suffered from 'Gesichtsrose' (erysipelas) and when they had last seen her was too ill to be moved. She was presumably still there and would, they thought, be glad to be evacuated out of the way of the Russians. [Comment: this reason for evacuating Frl. Hagen was not suggested by the interrogator.]

41d. When asked to describe her they all agreed that she was tall, fair-haired and anaemic-looking, walked with a characteristic stoop and had a high squeaky voice. Age about 38.

41e. Frau Dr. Hühnke was very worried at the probable fate of her mother and infant son Horst in a Russian occupied area. The interrogator did his best to calm her.

41f. The meeting was adjourned, its object achieved. The information was telephoned from Nightingale Lane to A.D.(C.C.R.) and TICOM representatives. [Comment: Frl. Hagen has since been evacuated from Zschepplin to Marburg where she is in hospital under supervision.]

Fourth Meeting; held at the Oratory School on 19th May, 1945 at 11 a.m.

Present: Prof. Vincent (in the chair), Major Seaman U.S.A., Lt. Fehl, U.S.A., Dr. Forster.
and later: Dr. Kunze, Professor Rohrbach, Herren Rave, Hierer and Grosse.

42. Dr. Kunze and Professor Rohrbach were called.

43. When examining the captured material it was found that the most recent work reports were missing. The gentlemen were asked what the explanation of this was. They replied that all the documents of the research section had been destroyed at Zschepplin.

44. Dr. Kunze was then asked about the machine, mentioned at a previous meeting (see para. 24), for solving the American strip. This machine was for decoding, not for analysing. Double-length strips were hung on lugs attached to rollers. The cypher text was typed on a machine which unrolled the strips so that the cypher text was visible along the bottom of the window. The clear text was then visible on some line higher up in the window. An electric device had been designed to illuminate the frequent clear text letters. This was abandoned, as it was found more convenient to print the common letters in heavy type on the strips and read off the lines containing the greatest number of letters in heavy type. The strips were made 52 letters long and were arranged in a bank of 15. The machine was thought to be with some Hollerith machinery in two waggons which had never arrived at Zschepplin. [Comment: see para. 24.]

45. With respect to the Hagelin Machine found among the captured material, Dr. Kunze said it was thought that Roumania, Sweden and Finland used this machine. No traffic had ever been solved for lack of time and personnel. He had heard it said that the Hagelin was also used by the French and American armies. The specimen mentioned had been acquired by the organisation for general investigation of its properties and had never been used to decode anything. [Comment: the number on the cyclometer of the machine is only 295.]

46. Dr. Kunze was then asked about the Japanese machine traffic discussed at a previous meeting; (see para. 19) and whether a machine had been constructed to decode it. He replied no, that they had been able to achieve the desired result with paper models.

47. Major Seaman then asked about the purpose of a number of rotary switches found among the captured material. Dr. Kunze said that he was not quite sure what switches were meant but he thought that they were captured material ('Beutematerial') sent to them 'in case they came in useful', as electrical fittings of this kind were in short supply.

48. Scandinavian systems were next discussed. No material had been read. Swedish traffic, thought a priori to be Hagelin, was investigated for three months in 1941. At first the machine had 25 letters, then after two months a machine with 26 letters was introduced. In August 1944 another investigation was begun, in which Professor Rohrbach participated, to determine whether the indicators fitted the Hagelin pattern.

49. Asked about Turkish systems, on which there was a noticeable lack of material among the captured documents, Dr. Kunze stated that all the Turkish material had been burnt.

50. Dr. Kunze was then dismissed and Messrs. Rave, Hierer and Grosse were called. Professor Rohrbach in the meantime explained that these gentlemen were of a definitely lower grade and had come to 'Pers ZS' to be trained. He spoke of them with obvious distaste.

51. Messrs. Rave, Hierer and Grosse were all employed by the O.K.W. and loaned to 'Pers ZS' in December 1943 to assist with Chinese and Japanese traffic.

52. Rave had joined the O.K.W. in October 1941. He was first at Tirpitzufer 72 - 76 until it was bombed out, then at Im Dol, Dahlem. He had got his friend Hierer into the O.K.W. because of his knowledge of Chinese. Grosse had been employed on Italian at the O.K.W. and was later transferred to Chinese. It did not appear that he had any knowledge of the latter language.

53. Rave, the spokesman of the group, gave a sketch of the organization of O.K.W. Chi. The head was Oberst Kempf, who was relieved in 1943 by Oberst Kettler. The sections were: translating and bookbreaking, under Ministerialrat Fenner; Interception; Intelligence, under Oberst Kalkstein; cryptographic research under Dr. Hüttenhain; and 'Z', the department dealing with administration and personnel.

54. Rave and the others had worked in Fenner's section under Oberleutnant Adler. This group consisted of 12 - 15 people, engaged at first on Japanese only, then Chinese.

55. When asked what htey had heard of notable successes of O.K.W. Chi, they said that they had heard vaguely of successes on American and British systems and mentioned American military attaché recyphered code read in 1942 when Rommel was in North Africa. They thought it had been broken by cryptography, not owing to physical compromise. [Comment: it was plain that these statements were based on rumour only.]

56. They admitted that most of the work done in 'Pers.ZS' was duplicated in the O.K.W., which worked on diplomatic systems only. Service systems were dealt with by the respective services concerned, O.K.H., O.K.M. etc. Liaison between O.K.W. and 'Pers.ZS' was carried on by Fenner and Paschke [Comment: Kunze and Paschke had been military cryptographers in World War I.], who were concerned at the amount of duplication and worked at avoid it. Their efforts were not regarded with favour by Selchow. There had been some co-operation, early in 1943 on Turkish, but apart from that the loan of Rave, Hierer and Grosse to 'Pers.ZS' had been the only occasion they know of on which the two departments had worked together. The situation was not improved by O.K.W.'s practice of calling up competent people from other departments, putting them in the ranks and then drafting them into its own cryptographic organization.

57. The O.K.W. had neither the long tradition nor the expertise which 'Pers.ZS' possessed, though Ministerialrat Fenner and a small party had been engaged on this work in peace-time. [Comment: it is possible that this was said in deference to Professor Rohrbach who was present throughout this interview.]

58. In the matter of captured material and machines, Rave said that new arrivals at O.K.W. Chi had been shown a British machine captured at Dunkirk. It was broken and rusty and did not work.

59. Chinese and Japanese systems: They had read a Chinese Military Attaché system, which had ceased in April or May 1943. The first groups of the traffic were EFR, SKW or JKW. The recypherment consisted of transposition within the code groups. The groups were 3 letter groups. They solved the recypherment but never read any messages.

60. Another Chinese traffic, with descriminant NKDEN, was investigated. It also consisted of 3 letter groups but was unrecyphered. It contained many spells which were easily recognisable, the names etc. being spelt out in simple substitution. It was a purely military code.

61. They broke a Japanese 'Kennwort - Code' consisting of double transposition of 2 and 4 letter groups from a known book; the transposition was done by a stencil, the stencil being the same for both transposing operations. The system was broken on a re-encypherment. It was a diplomatic system used between Moscow and Tokio. They read it from the middle of 1942 to June or July 1943.

62. No work was done on Japanese attaché systems. Rave remembered the Japanese Naval Attaché visiting Oberst Kettler.

63. Grosse, asked about Italian work in the O.K.W., mentioned a diplomatic system AR 22 and the Impero code as having been solved. His statement in general tallied with that of Dr. Paschke at a previous meeting on Italian work in 'Pers.ZS' (see para. 25) The Italian section in the O.K.W. consisted of 15 to 17 people.

64. Professor Rohrbach pointed out, after these gentlemen had been dismissed, that their statement on the Japanese 'Kennwort - Code' had been inaccurate. The recypherment was single transposition, not double.

Fifth Meeting; held at the Orm by School on 19th May 1945 at 3 p.m.

Present: Prof. Vincent (in the chair), Major Scumm U.S...., Lt. Fehl, U.S...., Dr. Forster.
and later: In succession: Dr. Karstien, RR. Zastrow, Prof. Rohrbach

65. Dr. Karstien and Professor Rohrbach were called together. Dr. Karstien however objected to the presence of Rohrbach and it was agreed to interview him alone. [Comment: Rohrbach informed the meeting later that there was considerable antagonism between himself and Karstien.]

66. Dr. Karstien had been employed on Slavonic systems until 1930 when he changed to Chinese. In 1938 after the Anschluss the Slavonic countries became more important and he went back to them.

67. The Yugoslavs used a five figure code with letter bigram tables consisting of 100 bigrams. This system was read from 1938 to 1943, when traffic dropped, after which it was read with interruptions. They had not received any Tito traffic, nor military attaché.

68. Arising out of the matter of attaché systems he gave a short summary of the division of work between the O.K.W. and 'Pers.ZS'. The O.K.W. had at first been responsible for service systems only but had not had enough readable material to train its personnel. It had then taken up diplomatic systems and having once tasted blood it refused to leave them. 'Pers.ZS' left all attaché systems to O.K.W. [Comment: Dr. Karstien was clearly at some pains to bring out the interdepartmental rivalry at which other members of the organization had only hinted.]

69. He mentioned a 10,000 group Chinese Code worked on by Dr.Olbricht, who he thought was lucky, as in the days when he himself worked on the Chinese he had to cope with a code book of 40,000 groups.

70. Asked about the application of the experience of the organization to the security of German systems, he said that at an early stage the Germans had progressed so far on a scientific basis that they had little to learn (... 'sind schon früh auf wissenschaftlichen Gebiet sehr weit gekommen, sodass wohl kein Belehrung nötig gewesen'). He mentioned O.R.R. Langlotz (who died two years ago) and O.R.R. Schauffler as having materially contributed to this desirable result. [Comment: see para. 117.]

71. He discounted any assistance received from captured material. He had had occasion to examine captured Czech material and stated that the Czech systems were unbreakable. In reply to the question (in what respect were they unbreakable? he stated that the Czechs used one-time pads. There was, he explained, a difference between systems which were insoluble in practice (owing to lack of time, personnel or equipment) and those insoluble in principle, such as the Czech, Russian and German systems. [Comment: This valuable distinction was much appreciated by the interrogators.]

72. Polish systems he had found unbreakable in practice; there were too many of them. They required more labour than the department had at its disposal. He mentioned a five figure book with a subtractor.

73. The Bulgarians used five figure books of 40,000 groups with frequent repetition.

74. The Lithuanians on Lotta used mainly transposition, sometimes double, sometimes single, occasionally encyphered with Vigenère substitution.

75. He had never been concerned with the solution of machine systems.

76. No liaison with foreign cryptographers existed.

77. No intelligence work was done in the department itself on decyphered material, though the selection of material for issue was of course guided by considerations of its possible intelligence value. This selection was done by the Referent [sub-section head] on the basis of knowledge and experience.

78. In the matter of official recognition of work done by the organization he observed that there was none, even from the Minister though, as everywhere, the authorities were quick enough when it came to complaining. [Comment: this question was inspired by the discovery in Dr. Paschke's private papers of a letter dated 30.5.1938 from the Foreign Minister, von Weizsäcker, congratulating Paschke on particularly successful efforts ('besonders erfolgreiche Bemühungen') in the field of work assigned to him.] 'We worked', said Dr. Karstien with some complacency, 'entirely in the dark' ['Wir arbeiteten vollständig im Dunkeln'. Comment: the romantic aspect of this kind of activity appeared to afford him some satisfaction.] It had been different with the Austrian Foreign Office cryptographers, who had been paid partly by results; solution of a difficult problem had been rewarded by a bonus. A former member of the Austrian organization (now dead) had transferred to 'Pers.ZS' after the Anschluss and professed himself dissatisfied with the remuneration in his new employment.

79. Dr. Karstien was dismissed and Herr Zastrow called.

80. Herr Zastrow asked that Professor Rohrbach be allowed to be present at the interview. He was accordingly called.

81. Herr Zastrow is a bookbreaker and has been engaged on U.S. systems for 27 years. The Americans used mainly 5 letter books with 10 recyphering tables for monoalphabetic and bigram substitution to each book. The tables run for two to six months. Later other substitution tables began to be used, with 5 indicator groups [illegible] table. The tables were changed in the course of a message, the indicator for the new table being encyphered with the previous table.

82. The german designation for these systems was B1, B2, B3 etc., to B10, (B = Buchstabe). American equivalents he remembered were:

16a = A1
16b = B1
37 = C1
M6 = Brown Code

The M6 book was known through physical compromise. The 'Brown Code' had been captured but it had been broken before capture. The reconstruction of the book had taken 2½ years.

83. ... transpositi n system used by the 'Coordinator of Information Washington' was mentioned. No success had been achieved with this.

86. At one [illegible] Herr Zastrow had been lent to the O.K.W. The head of the British and American subsection in the O.K.W. was C.V. Rohen, who did the same work as was done in 'Pers.ZS' but had more people to [illegible].

86. Herr Zastrow knew of no U.S. machines or cyphers other than the strip.

86. He said that he was tired of cryptography after 27 years and would like to change over to some kind of administrative post in the diplomatic service. [Comment: the interrogators did not think he would do well in such a post!]

87. Professor Rohrbach was careful to point out that the loan of Zastrow to the O.K.W. by 'Pers.ZS' was a very different matter from the loan of Rave, Hierer and Grosse to 'Pers.ZS' by the O.K.W. Zastrow was an expert and a man of considerable experience, whereas the other three were young men who had to be taught their business. [See para. 50]

88. [Comment: Conversation was carried on in English. Herr Zastrow's speech consisted largely of indistinct mumblings, so that some difficulty was experienced in recording what he said. Prof. Rohrbach informed the interrogators that Zastrow was very difficult to understand even when speaking German.]

89. The meeting was adjourned.

<u>Sixth Meeting; held in the Oratory School on May 21st, 1945, 11 a.m. to 1 P.M.</u>

Present: Professor Vincent (in the chair), Commander (S) Dudley Smith, R.N., Major Seaman U.S.A., Lt. Fehl, U.S.A., Dr. Forster, P.O.M. Phipps W.R.N.S. Dr. Paschke, ORR Scharffler, Prof. Rohrbach.

90. The main object of this meeting was to obtain information on work done on British systems.

91. In reply to the question whether work was done on Colonial Office, Dominions or India Office systems, <u>Dr. Paschke</u> replied that it was difficult to keep them apart. All unrecyphered codes were investigated. India Office traffic was only investigated when enough material was available, which was not often, and in any case there was little material.

92. <u>British unrecyphered 4-letter books.</u> The time lag between the introduction of a new book in the reading of enemy traffic naturally varied very much, but in favourable circumstances was of [illegible] months. Much of course depended on [illegible] link-up with [illegible] in the [illegible]. They had a subsection for reading messages for this purpose but information from the press could [illegible] if the book was [illegible] to some extent and was then rapidly [illegible] partially [illegible] was found to be based on such material. The [illegible] system which the books were constructed was a substitute in their reconstruction.

93. British unrecyphered 5-letter books. The time lag in book-building was longer than with the 4-letter books, i.e. 4 to 5 months, but the content of the messages was less important. There were two large books, one in general use, the other principally used for the traffic traffic of the South Africa Government. The first was also used by Eire. These books were of no great importance and were not fully built up.

94. One 4-letter and one 5-letter book were captured in Norway but both were already readable.

95. No recyphered letter traffic was read.

96. British figure systems. They had no captured books, but an out of date recyphering table was captured in Norway, which enabled Dr. Kunze to strip the traffic for a time. Analysis of the captured table gave an idea of the scope and method of recyphering, but they never actually read any of the traffic. The starting points for the subtractor depended on the date and the number of the message.

97. No work was done on figure traffic sent with a 5-letter indicator of the type CVCVC or VCVCV. It contained groups on unrecyphered code in the preamble. No intelligence about order of battle of military authorities etc. was extracted from these preambles in the Auswärtiges Amt, as the O.K.W. had copies of the messages in any case. No assistance in breaking additive recyphherments was received from references to previous telegrams made in plain code in the preambles of cypher telegrams.

98. A "five" figure system, Interdepartmental Cypher, was captured in Norway, but the O.K.W. and Görings Forschungsamt were principally concerned with its exploitation. He thought that the degarbling system had been reconstructed.

99. Dr. Paschke made it clear that although these systems were notrread, there was in fact enough material for them to be readable. When asked whether any assistance was offered the organization in this respect he said that they had to manage with the personnel they had. The requisition of Hollerith machinery had no connexion with the previous failure to solve British systems. Periodical checks were made to see whether the systems changed but they were convinced that no fundamental change occurred.

100. No work was done on British commercial or Bank of England systems. Dr. Paschke was of the opinion that these were not handled by the O.K.W. either and suggested that Göring's Forschungsamt might have been concerned, as it had economic and industrial interests.

101. Authorities responsible for cryptographic work on diplomatic material: It was made clear at this point that there were three independent parties working on diplomatic systems in Germany - the O.K.W., the Auswärtiges Amt, and Göring's Forschungsamt. The Auswärtiges Amt had less liaison with the Forschungsamt than with the O.K.W.

102. Shift Working: Working hours were from 8 a.m. to 8 p.m., though Dr. Kunze's party occasionally worked nights. There was always a duty officer available at night. They had no regular shift system because it was difficult to get people who were suitable to be keen at watches.

103. Interception: Material came from main sources:

1. O.K.W., which maintained interception stations in Lwuf, Treuenbrietzen and Wünsch. Traffic received by L/T.

2. Forschungsamt, [illegible] unknown. Material intercepted by the Post Office, both W/T and L/T, reached 'Pers.ZS' through the Forschungsamt until that was bombed out, after which this type of material came direct from the Central Post Office.

3. 'Pers.ZS' maintained a small interception station of its own in Dahlem, called Landhaus. It was used to cover the more important traffics such as Ankara and Lisbon. London was always very poorly received.

104. The O.K.W. maintained interception stations in occupied countries; he knew of one in the Balkans, one in Greece and one in France. No material was received from diplomatic posts abroad and none from foreign interception services, except some traffic intercepted by the Hungarians which was forwarded through the O.K.W. Nothing was ever received from the Italians or the Finns. In most cases the traffic was copied in the O.K.W. or the Forschungsamt before it reached 'Pers.ZS', so there was no indication of its origin.

105. It was stated that the O.K.W. did no work on British recyphered books.

106. If when a new system was broken it was discovered that traffic dealt mainly with matters outside the diplomatic field, it was handed over to O.K.W. for exploitation.

107. Dr. Paschke was unable to say which British channels produced the greatest number of messages with intelligence value and said that Frl. Hagen could answer this question precisely. [Comment: See para. 41a ff; this lady is ill and is at present detained at Marburg.]

108. On the matter of misuse of low grade systems for the purpose of passing high grade information, Dr. Paschke stated that though in general the intelligence value of the low grade traffics was not high they had carried a number of messages of considerable interest. His impression had been at the time that these messages were passed in that way for the express benefit of the Germans. He recalled a number of messages before the out-break of the war to the effect that Britain would not remain neutral in the event of a conflict between Germany and [illegible]. He referred to a case about six months ago of a cipher telegram from London to Berne concerning the burning of a signature to the [illegible]. This message caused considerable interest in Berlin [illegible] cryptographers were asked to check its accuracy, as its meaning was not clear. There was no cryptographic uncertainty about the decypherment, but the recipient's request and its meaning was never cleared up. One such messages were shown to the Führer, principally those concerning the treatment of prisoners of war.

109. [illegible] prefixed "HYM" was read.

[illegible] American traffic: More importance was attached to American than British traffic, until [illegible] cryptographers, as the American material was easier to read. The links to Berne, Ankara, Lisbon and Vichy were the most important, Stockholm also so. The Berne link passed messages from agents in Germany. Intelligence material was also passed from Finland to Moscow.

111. ORR. Schauffler was asked about his interest in cypher machines. He said he never used any himself, but collected material bearing on the subject.

112. As much as twenty years ago he was interested in the Enigma as a cryptographic device. He mentioned a printing Enigma as existing in those days, which was superseded by the Enigma with lights. The Wehrmacht had taken up this latter model and improved it.

113. The commercial type Enigma used by the Swiss was sometimes solved by stereotyped beginnings and known settings. The Swiss used to include in their messages the machine setting for the next message.

114. He had investigated the Kryha machine and had reported that it was soluble.

115. He had also some knowledge of the 'Geheimschreiber', one of the principal features of which he described as consisting of wheels with adjustable wiring. It was not very satisfactory and Hüttenhain of the O.K.W. Forschungsabteilung [Comment: not to be confused with Göring's Forschungsamt] was continually finding cryptographic faults in it. The Auswärtiges Amt used the 'Geheimschreiber' but the O.K.W. was responsible for the security of the device.

116. When asked where the machines came from which 'Pers.ZS' investigated, he said that they were supplied in order that their security could be tested. Hagelin machines had been investigated by the Wehrmacht and O.K.H. had read material encyphered with them.

117. His own special duty was to ensure that cryptographic possibilities were known and appreciated. He had worked with ORR. Langlotz (see para. 70), Head of the Cypher Security Section of the Auswärtiges Amt, on this subject and was satisfied with the liaison existing with the authorities responsible for German systems.

118. At this point, Dr. Paschke observed that they 'had reason to be convinced of the superiority of German systems' ('Wir waren mit Recht überzeugt von der Überlegenheit der deutschen Verfahren'), with which ORR. Schauffler agreed [Comment: the general context of this remark suggested that 'German systems' was intended to include the machine systems used by the armedforces.]

119. In reply to the suggestion that the advent of machines meant that the great age of cryptography had come to an end, ORR. Schauffler said that the great age had begun with the first world war and was likely to end with the second. It was however worth bearing in mind that at the end of the last war people were saying that the use of cryptography was over.

119a. He felt that the history of cryptography, in which he had a life-long interest, had in this connexion a real function to perform, in that it attracted attention to methods of solution and general cryptographic possibilities. Machines for instance were only insoluble as long as they were well used. The Swiss Enigma had been read because it was badly used. The Germans had laid down strict rules for the use of the Enigma to ensure that compromise did not occur through improper use. The same applied to other systems.

120. Dr. Paschke on this point spoke of a Russian diplomatic one time pad which had been used by the Russian army under conditions which did not permit the normal instructions for use to be observed and which was thus compromised. The O.K.H. had read it up to Stalingrad. The pads were used more than once. The traffic was read currently on the basis of frequent repeats of texts. The solution was helped by the circumstance that the Russians always used diplomatic texts, as their belief for security in the encipherment. The diplomatic pads are all four figure, the army pads all five figure.

121. Special characteristics of Russian one time pads. Large differences between adjacent figures were conspicuously rare. He had seen specimens of Russian one time pads captured in the field. They had been typed on a typewriter with one carbon. Series of figures (e.g. 345678 etc.) with a difference of 1 were common and other psychological peculiarities of the typist, such as a recognisable instance for zero ('angst vor dem Null'). The indicators were encyphered with the first group of the finished telegram. The false sum if the penultimate group was the discriminant.

122. Mentioning the circumstance that the Russian systems changed after the publication of the British White Paper in 1927, ORR. Schauffler remarked that we did not publish the really interesting material at the time and he had never been able to understand why not.

123. Double transposition. When asked about their general success with systems of this kind, Dr. Paschke stated that it was sometimes possible to read them currently, but that it depended on the number of keys. In general he thought, and ORR. Schauffler agreed, that they caused as much trouble to the legitimate users as they did to the cryptographer; they were secure but laborious. American double transposition systems were known to exist, but no work had been done on them.

124. Last War Papers: ORR. Schauffler observed that his boxes among the captured material ('Serie 20') contained a collection of material relating to the cryptographic work done by the Germans on British naval ciphers during the last war.

125. Summary of the organisation since its Inception: Rough figures were given as follows:

1940	20 to 30 people
1941	50 people
1942	80 to 100 people
1943	150 to 200 people

126. The meeting was adjourned. Ref to the adjournment Professor [illegible] whether anything could be found about the Romanoff, the 'Tsar.s' codelist on Turkish, Polish and Slavonic countries, which had been last heard of in custody of allied Military Government police. He was also anxious to have news of the state of health of Mr. Crumbly, who is now in hospital. The meeting was unable to provide information on either of these points.

Seventh Meeting; held in the Oratory School on May 21st, 1945. 2.45 p.m. - 6 p.m.

Present: Professor Vincent (in the chair), Cdr (S) Dudley Smith, R.N., Major Seaman U.S.A., Lt. Fehl, U.S.A., Dr. Forster, P.O. M. Phipps W.R.N.S.
and later: Professor Rohrbach, Dr. Schroeter, Dr. Schultz, Herr Krug Herr Brandes, Dr. Benzing, Dr. Deubner, Dr. Olbrecht, Dr.Müller

127. On the advice of Professor Rohrbach it was decided to divide up up the eight members of the party who had not yet been interviewed into three groups, taking the three gentlemen from Dr. Kunze's party first. It was pointed out to him that the restricted accommodation available did not enable the meeting to ask him to 'sit in' on the interviews, as had been done on previous occasions, and that the presence of section heads at the interviews of members of their sections, which he earnestly requested, would be impossible for the same reason.

128. Dr. Schultz, Dr. Schroeter and Herr Krug were called.

129. Dr. Schultz is a mathematician and statistician by profession. He worked before the war in the Statistisches Reichsamt and was transferred to Dr. Kunze's part in 1939 at the outbreak of hostilities. He had worked on the Japanese machine until 1940 when it ceased to be soluble. It had been broken before he came to work on it.

130. He then worked on the American B7 (C1) code and solved the recypherment. There were 80 to 100 tables, the first of which were difficult to reconstruct, the later ones getting progressively easier. He built up 80 tables himself. When the tables changed, so that the sequence was no longer cycvc, he continued investigations, but work was discontinued in favour of the American strip '02'.

131. He had assisted Dr. Kunze with investigations on the Enigma machine, and the Swiss enigma was successfully solved.

132. He stated that his interest in these matters was purely theoretical and mathematical and that he had little idea of the intelligence value of the material he investigated. It usually left his hands before it was actually readable, as Dr. Kunze's party was responsible primarily for breaking recypherments.

133. When asked what he considered the greatest methodological achievement of Dr. Kunze's party during his term of service, he said that the '02' American strip was in his opinion the greatest success. It was solved by hand, as at that time they had no machines. ('02 wurde entschlüsselt ohne jegliches Hilfsmittel'). He sketched the method of solution as follows:

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958.

135. In the autumn of 1944 he had begun work on a Polish system, a 4 letter book enciphered with bigram substitution. This system had been investigated before but work on it had been discontinued for a while. Göring's Forschungsamt had been interested in it but had not seriously tackled the decypherment and had restricted itself to sorting the material. This system was used by the Polish Government in London for communication with Berne, Washington, Cairo and Jerusalem. He had seen no traffic between London and the underground movement in Poland. Dr. Kunze's party was still working on this system at the time of the capture of Zscheppin. Some tables had been recovered and related, but no book-breaking had been done.

136. Dr. Schroeter: Had joined the organisation comparatively later (Göring 1941) and had no intention of 'staying on'. He was a lecturer in mathematical logic at the University of Münster. He had joined Dr. Kunze's party and worked independently on Japanese decypherments.

137. He started work on simple transposition decypherments of codes;

140. Herr Krug is a mathematician and a school-master by profession, who had joined the organisation in 1940.

This is a copy
The original has
been retained under
section 3(4) of the
Public Records Act
1958

This is a copy
[illegible] has
been [illegible]
[illegible] the
[illegible] Records Act
[illegible]

old. All this time they had no machines and all work was done by hand.

142. They read no traffic prefixed INDIV, INLEK or AFAR.

143. Hollerith machinery: When Hollerith machinery was finally required Herr Krug was put in charge of the subsection which operated it. In reply to the suggestion [Comment: see comment on para. 23] that the acquisition of Hollerith machinery was in some way connected with the failure to continue reading British systems, Herr Krug said that there was no connexion. His next-door neighbour in Berlin-Lichterfelde was a Dr. Koch who was manager of the German Hollerith concern. Friendly conversation with Dr. Koch had set Herr Krug thinking about the application of this kind of machinery to his own work. He had put the project up to his superiors and in due course the equipment had arrived. [Comment: at the First Meeting Professor Rohrbach had suggested (see para. 6) that the acquisition of the machines was due to the personal interest of Ribbentrop]. He said that the OKW possessed no machinery of this kind, but that Göring's Forschungsamt did [Comment: there may be some confusion here between the Forschungsabteilung of the OKW and Göring's Forschungsamt].

144. The machines they had were:

20 'alphabetische Locher' (alphabet punchers)
10 'Sortiermaschinen' (sorting machines)
2 'Kartenmischer' (collators)
2 'Kartendoppler' (reproducers)
1 'Rechenlocher' (number punchers)[Comment: he said this was for multiplying and differencing]
4 'Alphabetische Tabelliermaschinen' (alphabetical tabulators)
2 'Tabelliermaschinen D 11' (calculating tabulators)
1 'Spezialvergleicher' (multipurpose machine designed by themselves)

145. They had designed a number of accessories to these machines. For the sorting machines, they had designed two devices: a 'Kartenzähler' [card counter] and a 'Nummernsucher' [number finder]. The alphabetical tabulators had an attachment which prevented the machine from printing unless there were two or more identical cards. This was useful for finding reports.

146. The 'D 11' machines were not Hollerith but ordinary statistical calculating machines made by a German firm. [Comment: the 'D 11' is a Hollerith machine. The captured material contains several prospectuses describing it]

---

146. The tabulators would print figures, but the calculating machines would not print letters.

149. Dr. Schultze, Dr. Schroeter and Herr Krug were dismissed and Herr Brandes, Dr. Benzing and Dr. Daubner were called.

150. Herr Brandes is a bookbuilder and joined the organisation in 1920. Since 1938 his special field has been the systems of France, Belgium and Switzerland. He was satisfied with his work on the whole but thought that more could have been achieved with more staff.

151. French: they had read recently a de Gaulle system consisting of a four figure book with a subtractor consisting of five digits repeated to the end of the message, changed daily. The code was a hat book which had been revised ('neugemacht') since 1937. It contained a group for 'Général de Gaulle', but this was a later alteration. Common significations had a number of alternative groups; 'du', 'de l', 'des', 'full stop' etc. had up to 10 to 20 groups. The traffic passed on this system was of a fairly high order. It was used with Washington, London, Stockholm, Moscow, Madrid, Chungking, Buenos Aires and Montevideo.

152. He spoke of another French system consisting of a four figure book with letter bigram substitution with limitations. Only 10 letters were involved, so it was easy to convert them into figures. The recypherment was done by tables of 100 bigrams, changing quarterly. The same table would be used on different dates in successive months of the quarter. The bigrams were taken horizontally. Only the Navy used horizontal and vertical substitution together.

153. He mentioned an unrecyphered book which was not broken. It ran concurrently with the system described above and had the same external characteristics.

154. There were several French systems which they did not read.

155. Belgian: They knew four different Belgian systems.

156. The first was a four letter book, used in two forms:
1) a straight alphabetical vocabulary, in which e.g. 'full stop' = UYAK, or 2) in which the groups were transposed within themselves and UYAK was expressed as KUYA. The latter form was the commoner. This book was used with daily changing bigram tables. At first these tables were systematically construct but grew progressively less so until they were finally not systematic at all.

157. The second was a three letter unrecyphered book on which they did not work.

158. The third was a book known to them as KAMI (the code group for 'full stop'). If the groups were rearranged in the form MIKA the book was partly alphabetical. It was recyphered in the same way as the first (KUYA/UYAK) system.

159. The fourth was a four figure code used for traffic with the colonies. The recypherment consisted of transposition of one half of the book group and substitution of the other half. This code could be used as a five figure book, in which case the significations in the second column had to be taken. All the traffic on this book was read.

160. Swiss: Everything was read except the machine, and that was readable for a time.

161. There was a 3 letter code with recypherment by substitution in columns, separate tables being applied to a single letter and the two subsequent letters. The recypherment changed after the 11th,

15th and 26th groups; a letter, recyphered with the previous tables, indicated which tables were to be used for the following groups.

162. He mentioned the 'HE 3' code, a trilingual book with German, French and English editions. An indicator showed which edition was being used. This book was unrecyphered.

163. Dr. Brandes was unable to state the exact dates when the Swiss Enigma was read but said that it was read completely for a considerable time. [Comment: the phrasing of his statement implied that there was also a time when it was partially readable].

164. Dr. Benzing joined the organisation in 1937. He is an orientalist by training, Turkish being his speciality. He worked as a bookbuilder on the systems of the Near Eastern countries. His section was fully occupied with Turkish and Persian, so that although in theory they were also responsible for the Arabic speaking countries, no work was in fact done on them.

165. All the Turkish diplomatic traffic was read. A few short messages sometimes proved difficult. The Turks used a 40 figure subtractor.

166. All the Persian systems were read. They used a three letter book with substitution tables, which often changed. The Persians however always indicated in clear which table was in use.

167. Dr.Deubner: a classical archeologist by profession [Comment: of considerable repute]. Had done excavations in Greece and had a post at the Pergamon Museum in Berlin. Worked on Italian and Greek systems.

168. Italian: asked about Italian systems after the collapse he mentioned a double transposition used by the Badoglio government which was never solved, and a readable unrecyphered letter 'administrative code' used mainly for communications with Berne, and a system known to them as the 'Salzburg-Verfahren' with a 10,000 group ('Element') subtractor. This system was very difficult and was worked on by Dr. Paschke personally. It was seldom broken.

169. Greek: there were three systems, all of which were read:
1) a clear 5 letter book, the fifth letter of which was dummy; this carried most of the traffic.
2) a clear 4 letter book, used mainly for traffic with Berne.
3) a four figure book used with bigram substitution of 30 tables of 100 bigrams each. It was used between London and Moscow, Washington, Cairo and Ankara. Traffic from London amounted to about 1 a day. The bigram tables changed according to the date.

170. They had not received any captured Greek code or cypher documents.

171. They had read no partisan traffic.

172. He stated that there was close liaison with the O.K.W. in his field to eliminate duplication of work.

173. It took up to 8 days to receive traffic from intercept; and from 1 to 4 more days before translations were issued.

174. Herr Brändes, Dr. Benzing and Dr. Teubner were dismissed and Dr. Olbricht and Herr Müller were called.

---

175. Dr. Olbricht is a bookbreaker. He took a doctorate in Chinese in 1938 and joined the organisation in 1939, where he worked mainly on Japanese and Manchurian systems.

176. JB 57. Another Japanese two letter book with a recypherment consisting of stencil transposition with mills, which was read for about two years. There was also a variant with substitution recypherment using a table of about 30 alphabets.

177. He confirmed Dr. Schroeter's statements on Japanese systems.

178. Manchurian systems: he mentioned transposition recypherments of a basic Japanese three letter book. There were 366 very small cages, one for each day. If the message was too long to fit one of these cages, it was continued on the cage for the next day and so on. This system was no longer current. Dr. Schroeter had been working on a current Manchurian system, the method of recypherment of which was thought to be the same as before.

179. They had had a captured Manchurian code book.

180. They did not handle Chinese military attaché traffic. A Chinese system called UTI had been solved in 1941-42.

181. Dr. Müller is a private teacher of languages who joined the organisation in 1940. He worked on Scandinavian and American systems.

182. His work on Scandinavian lasted for three months in 1940 when all Scandinavian work was transferred to the OKW. During that time he had worked on a Swedish unrecyphered five figure hat book. Practically no work was done on Danish or Norwegian. He had some unofficial liaison with people at Göring's Forschungsamt who were working on Scandinavian.

183. After he gave up Scandinavian he worked on U.S. systems and corroborated in general the statements of Herr Zastrow on these (see para. 80 ff.) He added that the 'Brown Code' was used for traffic with Berne, Ankara, Kuibyshev, Beyrouth and South American posts such as Rio de Janeiro. He knew of no American system B9 or B10.

184. The meeting was adjourned.

Interrogators' Personal Impressions of Principal Members of 'Pers.Z'

185. Professor Rohrbach: Heavy diplomatic manner. Forceful character. .. schemer. Hoped to sell 'Pers.Z' as a going concern to the Western Allies. Speaks some English.

186. Dr. Paschke: Has more dignity than the others. Very diplomatic manner. Has careful to say no more than circumstances demanded. Put up a good show. Heavy type. Speaks some English.

187. Oberregierungsrat Schauffler: Said as little as possible and moreover has difficulty in expressing himself. Appears to be asleep most of the time; this is deceptive. Unworldly academic type. Greatly respected by his colleagues. Understands English.

188. Dr. Kunze: Professional competence apart, rather nondescript. Anxious to please, but often gave evasive answers.

189. The three section heads were obviously prepared for thorough cross-examination, and were somewhat nonplussed by the informal way in which the interrogation developed. Such information as was withheld by the seniors, or rather was not volunteered by them, was, however, easily obtained from subordinates.

190. Dr. Karstien: Cold, dandified and conceited; a 'man of the world'. Had a low opinion of the interrogators, which was reciprocated. Likely to be more affected by intellectual than by moral scruples.
Understands English.

191. Dr. Schroeter: Pleasant academic type, good character.

192. Dr. Schulz: Unworldly academic type; rather frightened of us.
Some English.

193. Herr Krug: An enthusiast for his job, particularly for his machines, and eager to talk about them.
Some English.

194. Frl. Friedrichs: [illegible] woman of [illegible] character, who would [illegible] the top in any profession. Probably not to scrupulous. Probably in any dubious undertaking.
English fluent and idiomatic.

195. Cover Names used during the interrogation:

Tiltman	=	[illegible]
Vincent	=	Wilson
Cook	=	
Seaman	=	Seymour
Fehl	=	Marshall
Dudley Smith	=	Anderson
Forster	=	Macgregor

A P P E N D I C E S.

A: Organization of 'Pers.ZS' as at end of 1943.
B: Organization of 'Pers.ZS' as in April 1945.

These are copies of documents compiled at the request of Lt.Col. Evans by ORR. Schauffler and Dr. Paschke.

A. ORGANIZATION OF 'PERS.ZS' AS AT END OF 1943

Auswärtiges Amt Dargscheidungen, den 27.April 1945

Abteilung 'Pers.ZS'

d.i.: Entzifferungsdienst für fremde diplomatische Telegramme mit der Bezeichnung "Sonderdienst", verwaltungsmässig der Personalabteilung des Auswärtigen Amtes angegliedert.

Leiter: Gesandter I.Kl. S e l c h o w

Ab Ende 1943 durch Verlagerung von zwei Abteilungen in Ausweichquartiere Aufteilung des Gesamtsonderdienstes in drei Abteilungen, die durch täglichen Kurierdienst miteinander verbunden waren. Dauer dieses Zustandes bis Januar 1945.+)

Hiernach war die Verteilung der Geschäfte wie folgt:

I. Stammabteilung B e r l i n - Dahlem

Leiter: Oberregierungsräte S c h a u f f l e r
und P a s c h k e

a) Schauffler:

1. Japan
2. Systematik und Grundlagenforschung
3. Verwertung der Erfahrungen an fremden Chiffrierverfahren für die eigenen Verfahren des Reichs

b) Paschke:

1. Verwaltung
2. Bearbeitung und Edition von diplomatischen Telegrammen folgender Länder:

a.	Japan, China	ORR Schauffler
b.	Türkei	ORR Scherschmidt
c.	Iran, Afghanistan	LR Dr. Benzing
d.	Italien, Griechenland	ORR Paschke
e.	Frankreich, Belgien, Schweiz	RI [illegible]
f.	Rumänien	LR Dr. Kemper
g.	Jugoslawien	Dr. Krummel
h.	UdSSR	Ostrop
i.	Skandinavien, Irland, Spanien, Portugal, Lateinamerika	Frl. Hagen

3. Information und Nachrichtenkartei Prof. Dr. Horn.

+) Ab Februar und März 1945 wurden weitere Verlagerungen der drei Abteilungen notwendig, durch die [illegible] der Bearbeitung [illegible] zum Teil [illegible] gewesen sind (siehe [illegible]).

III. Ausweichstelle H e r n s d o r f (Riesengebirge)

Leiter: Oberregierungsrat Dr. K u n z e
Bearbeitung schwieriger kryptographischer Probleme: Diagnose und Lösung neuauftretender Chiffrierverfahren, insbesonders solcher, die einen grösseren Personal- und Zeitaufwand oder auch die Verwendung technischer Geräte erfordern.

Ein charakteristisches Beispiel für die Zusammenarbeit der obengenannten drei Dienststellen stellt das Arbeitsgebiet Japan dar; während z. B. in einem bestimmten japanischen Verfahren die Erstlösung der Überschlüsselung in Herrnsdorf gemacht wurde (Dr. Schröter), erfolgte die laufende Lösung der weiteren Schlüssel in Hirschberg (Dr. Olbricht) und wurde schliesslich der zugehörige Code in Pahlen entwickelt, wo auch die Übersetzung und Auswertung der betreffenden Telegramme vorgenommen wurde (OKW Schauffler).

E. ORGANIZATION OF 'TBRS. B' AS IN APRIL 1945

'Tbrs.B' (Sonderdienst des Referats J in der Presseabteilung des Auswärtigen Amts)

Aufgabe: Auswertung der Arbeit diplomatischer Telegramme fremder Regierungen.

Leiter: Gesandtschaftsrat Dr. Schramm

Gliederung: (Stand vom April 1945)

I. Sekretariat, Grundsatzbearbeitung, Wissenschaftliches Archiv, Berichtswesen

Referent: [illegible]

II. Sprachlich-kryptologische Abteilung Leiter: ORR Paschke

A. Länder-Referate:

1. Frankreich, Belgien, Schweiz, Holland
Referent: RR Brandes
Vertreter: WHA Frl.Schrader

2. Britisches Imperium Irland, Spanien, Portugal, Mittel- und Süd-amerikanische Staaten, Thailand
Referent: WHA Frl. Hagen
Vertreter: WHA Frl. Wernick

3. Italien, Vatikan, Griechenland, UdSSR
Referent: ORR Paschke
Vertreter: WHA Dr.Doubner

4. Rumänien
Referent: RR Dr. Kasper
Vertreter: WHA Menning

5. Slawische Staaten (ausser UdSSR), Lettland, Litauen
Referent: RR Dr.Karstien
Vertreter: WHA Frl.Friedrichs

6. US, Skandinavische Staaten
Referent: WHA Dr.Mueller, Hans-Kurt
Vertreter: WHA Zastrow

7. Türkei
Referent: ORR Scherschmidt
Vertreter: WHA Burghard

8. Iran, Afghanistan, Arabische Staaten
Referent: RR Dr. Benzing
Vertreter: Frl. Dr.Schimmel

9. Japan, China, Manschukuo
Referent: ORR Schauffler
Vertreter: Dr. Olbricht

B. Büro, Information (Auskunftstelle für die Länderreferate) und Archiv der herausgegebenen Telegramme
Referent: Prof. Dr. Horn

III. Mathematisch-kryptologische Abteilung Leiter: OKR Dr. Kunze

Den 30. April 1945

INDEX

The numbers refer to paragraphs, not pages

A

Accessories to Hollerith machinery 145
Adler, Oberleutnant 54
'Administrative code', Italian - 168
Alphabetic tabulators 144
Alphabetische Locher 143
Alphabetische Tabelliermaschinen 144
Alphabet punchers 143
American 7 (C1) Code 129
American doubl transposition systems
American military attaché traffic 55
American strip 24, 30, 129
" , machine for solving 44
" , method of solution 133, 134
American systems 81, 110, 181, 183
AR 22 63
Arabic speaking countries 164
ARFIR 142
Attaché traffic 21, 68
" , Japanese military 21
" , American military 55
" , Chinese military 59, 180
Austrian Foreign Office cryptographers 78
Auswärtiges Amt 3, 101, 115, App.A
Austausch, einseitiger 12

B

B7 code 129
B9 183
B10 183
Bafoglio government 168
Bank of England system 100
Belgian systems 155 ff.
Benzing, Dr. 149, 164 ff., App.., App.B
Bigram substitution, American 81
" , French 15
" , Greek 169
" , Italian 25
" , Jugoslav 18
" , Polish 135
Bigram tables, Belgian 156
Bookbuilders 7
Brandes, Herr 150, App.A, App.B
British commercial systems 100
British diplomatic system 23
British figure systems 96
British Naval cypher, succes with - in 1914-18 war 14, 124
British recyphered books 105
British recyphered letter traffic 95
British systems 22 ff., 32, 55, 90 ff.
143
British unrecyphered 4-letter books 92
British unrecyphered 5-letter books 93
British weather cyphers 22
'Brown Code' 82, 183
Bulgarian cyphers 30, 73
Burghard App.B
Burgscheidungen 10, App.A

C

Cl code 129
Calculating tabulators 144
Captured material 26, 71
Card counter 145
Chiffrierabteilung 3
Chinese military attaché traffic 180
Chinese systems 20, 59, 69
Circular telegrams 16
Collators 143
Colonial Office systems, British 91
Comparator 147
'Coordinator of Information Washington' 83
Cover names used during interrogation 195
Cryptographers, foreign, relations with 9, 26, 76
- , Austrian 78
Cryptographic bureaux, liaison with 9
Cryptographic methodology 8
Cryptography 119
- , history of 119a
Cypher Security Section of Auswärtiges Amt 117
Czech systems 71

D

D 11 machines 144, 145
Dahlem 103
Danish traffic 182
Degarbling system 98
De Gaulle system 151
Doubner, Dr. 149, 167 ff., App. B.
Diplomatic Codes and Cyphers, Foreign 3
- , German 4
Dominions Office systems 91
Double transposition 123, 168

E

Eire 93
Enigma 112 ff., 119a, 131, 163
Evans, Lt.Col. 12, Appendices

F

Far Eastern languages 8
Fenner, Ministerialrat 53, 54, 56
Finland, use of Hagelin machine by 45
Forschungsabteilung, OKW 115
Forschungsamt, Göring's See under Göring's Forschungsamt
French systems 15, 150, 151 ff.
Friedrichs, Frl. 29 ff., App. B

G

Geheimschreiber 115
German systems, security of 70, 117, 118
Göring's Forschungsamt 98, 100, 101, 103, 115, 143, 182
Greek systems 167, 169 ff.
Grosse, Herr 51
Grundlagenforschung 8
Grunsky, Dr. 11, 126

H

Hagelin machine	45, 58, 115
Hagen, Frl.	32, 41a, 41c, 107, App.A, App.B
Hermsdorf	24, App.A
Hierer, Herr	51
Hirschberg	App.A
Hollerith machines	6, 23, 99, 143
Holloway Prison	41
Horn, Professor Dr.	App.A, App.B
Hühnke, Frau Dr.	41, 41c
Hüttenhain, Dr.	53

I

Identical indicators	141
IE 3 code	162
'Impero'	25, 63
India Office systems	91
Indicator, 5-letter, British figure systems	97
Indicator tables, American	81
INDIV	142
Intelligence	37, 77
INTER	142
Interdepartmental cypher	98
Interception	103
Italian systems	25, 167, 168
- , work on - in OKW	63

J

Japanese machine traffic	46, 129
Japanese military attaché traffic	21
Japanese Naval Attaché	62
Japanese recypherments	136
Japanese systems	18, 19, 59, 137ff., 175, 176f.
JB 57	176
JB 62	139
JB 64	138
Jugoslav traffic	18, 67

K

Kalkstein, Oberst	53
KMI	158
Karstien, Dr.	65 ff., App.A, App.B
Kartenmischer	144
Kartendoppler	144
Kartenzähler	145
Kasper, Regierungsrat Dr.	App.A, App.B
Kempf, Oberst	53
'Kennwort-Code', Japanese	61, 63
Kettler, Oberst	53, 62
Koch, Dr.	143
Krebs, Legationsrat	20
Krug, Herr	128, 140 ff.
Krummel, Dr.	App.A
Kryha machine	114
Kunze, Dr.	5, 6, 10, 11, 13, 30, 42 ff., 127, App.A, App.B

L

Landhaus	103
Langlotz, Oberregierungsrat	70, 117
Lauf	103
Lettish systems	74
Lithuanian systems	74
Lörrach	103
Low grade systems, British	108

M

Machine cyphers	8, 19, 45, 46, 111-119a, 129, 131, 160, 163
Machine for decoding Japanese traffic	46
Machine for solving American strip	44
Manchurian code book	179
Manchurian systems	16, 178
Menning, Herr	App.B
Methodology, cryptographic	8
Monoalphabetic substitution, American	81
Müller, Dr.	174, 181, App.B
Multipurpose machines	144, 147

N

Near Eastern countries	164
Neofascists, Italian	25
Norwegian traffic	182
Number finder	145
Number punchers	144
Nummernsucher	145

O

OKW	51 ff., 101, 105, 172, 182
OKW Chi, organization of	53
- , successes of	55
- , relations with 'Pers.ZS'	68
OKW Forschungsabteilung	115
OKW interception stations	103, 104
Olbricht, Dr.	69, 174, 175 ff., App.A, App.B
'One-sided exchange'	12
One-time pad, Czech	71
- , Russian	120, 121

R

Pannwitz, Frl.Dr.	41
Partisan traffic	171
Paschke, Dr.	5, 7, 25, 27, 33, 56, 78, 90, 99, 120, 166, App.A, App.B
Pergamon Museum	167
Persian systems	166
Pers.ZS	3, 56
- , organization of - as at end of 1943	App.A
- , - - - in April 1945	App.B
- , relations with OKW	68
- , strength of	125
Pers.Zs interception station	103
Polish systems	17, 72, 135
Portuguese systems	32
Prague	10
PRODROME	141

R

Rad 1	25
Rave, Herr	51 ff.
Rechenlocher	144
Recyphorments	6, 18
- , American system	81, 129
- , Belgian	157
- , Brit figure systems	96
- , Chinese system	59
- , Japanese	136
- , Japanese 'Kennwort-Code'	63
- , Manchurian	178
- , Polish	135
- , Russian	120
- , Swiss	161
Referent	77
Repaginstion in Bulgarian systems	73
Reproducers	144
Results, communication of	39
Ribbentrop	6
Rivalry, interdepartmental	33, 50, 56, 68, 87, 101
Rohen, Oberregierungsrat	84
Rohrbach, Professor Dr.	2 ff., 42, 48, 65, 127
Roumania, use of Hagelin machine by	45
Russian diplomatic one-time pad	120, 121
Russian systems	16, 120, 121, 122

S

Salzburgverfahren	168
Scandinavian systems	48, 181, 182
Schauffler, Oberregierungsrat	5, 8, 18, 20, 70, 111, App.A, App.B
Scherschmidt, Oberregierungsrat	126, App.A, App.B
Schimmel, Frl.Dr.	App.B
Schrader, Frl.	App.A, App.B
'Schriften des Sonderdienstes'	8
Schroeter, Dr.	128, 136 ff.
Schultz, Dr.	128 ff.
Security of German systems	70
Selchow, Gesandter	5, 8, 10, 56, App.A, App.B
Service systems	56
Shift working	102
Slavonic cyphers	30, 66
"Sonderdienst"	App.A
Sonderdienst des Referats Z in der Personalabteilung des Auswärtigen Amtes	App.B (See also Pers.ZS)
Sortiermaschinen	143
South Africa government	93
Sorting machines	143
Spanish systems	32
Spezialvergleicher	144, 147
Split repeats	141
Stammabteilung	App.A
Statistisches Reichsamt	129
Steinberg, Dr.	21
Strip system, American	24
Subtractor tables	17
- , British	141
- , Italian	25
- , Polish	72
Sweden, use of Hagelin machine by	45, 48
Swedish unrecyphered five figure hat book	182
Swiss commercial type enigma	113, 163
Swiss systems	160
Synthetics	141

T

Tabelliermaschinen D 11 144
Theoretical research 8
Translation of decyphered texts 38
Transpositions, use of machinery for solving 147
Treuenbrietzen 103
Trilingual book, Swiss 162
Turkish diplomatic traffic 165
Turkish systems 49
U.S. See under

U

U.S. See under American

V

Vigenère substitution 74

W

Weather cyphers, British 22
Wehrmacht, liaison with 7
Weizsäcker, von 78
Wernick, Frl. App.B
Women, position of - in organization 32

Z

Zastrow, Dr. 30, 79,ff., 183, App.A, App.B
'Z' department of OKW Chi 53
Zschepplin 24, 41c